



FEDERAL BUREAU OF INVESTIGATION

**FREEDOM OF
INFORMATION AND
PRIVACY ACTS
REFERENCE MANUAL**

PART 5 OF 9

MIOG SECTION 190

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

190-1 STATUTES

(1) The Freedom of Information Act (FOIA) should be cited as Title 5, USC, § 552.

(2) The Privacy Act of 1974 should be cited as Title 5, USC, § 552a.

190-2 ACCESS TO GOVERNMENT RECORDS

(1) The Privacy Act permits a U.S. citizen or permanent resident alien to access records maintained in a system of records by an agency of the Executive Branch of the Federal Government. Under the Act, only records about the person making the request can be accessed. A system of records is any procedure whereby information is maintained in a manner permitting retrieval by name or other personal identifier, e.g., records maintained alphabetically, rather than chronologically.

(2) The FOIA provides for access by any person to all information maintained by a Federal agency, e.g., information relating to individuals other than the requester, and information relating to some phase or phases of the agency's work.

(3) FBI files containing information compiled for a criminal investigation, including determining possible violations of the espionage and related statutes, are exempt from the access provisions of the Privacy Act; however, a release of such records may be required under the FOIA. This includes FBI criminal, counterintelligence, and terrorism investigations.

190-2.1 Exclusions From the FOIA

(1) "Tip-off" provisions in the FOIA allow the Government to treat certain records as not subject to the requirements of the FOIA. The provisions may be applied to a request which involves:

(a) interference with a pending criminal investigation when the subject of the investigation is not aware of its pendency;

(b) a request for records about an informant whose status as an informant has not been officially confirmed when the request is from someone other than the informant; or

(c) a foreign intelligence, foreign counterintelligence, or international terrorism investigation when the existence of the records is classified information.

(2) If the only records about the subject of the request are within the tip-off provisions, the response will be the same as if no record identifiable with the subject of the request was found. The response to the requester in both situations will be: "There are no records responsive to your FOIA request." [If some records about the subject of the request are within the tip-off provisions and some are not, the response will be: "The [records responsive to your FOIA request are ... " followed by a description of [the records not within the tip-off provisions.]

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

(3) FBIHQ approval is required prior to the use of the tip-off provisions. Approval is obtained by sending a teletype to FBIHQ, Attention: FOIPA Section Front Office, containing:

(a) sufficient information about each of the essential elements of the recommended exclusion;

(b) any additional information known about the subject matter of the request or the requester that might affect the decision;

(c) the caption and a brief description of the investigation to be protected, along with its current status, field office file number, and Bufile number if known; and

(d) the identity of the field office official recommending the use of the "tip off" and the person in the office to contact about the request.

A copy of the teletype should be sent to the office of origin and any other interested offices. If approval is given, the field office will notify the requester as indicated above in 190-2.1(2).

190-2.2 Time Deadlines

(1) A first-party request (an individual asking for records concerning himself/herself) requires that a determination concerning disposition of the request be made under both the Privacy Act and the FOIA. While the Privacy Act contains no time deadlines concerning access to records, the time limits for responding to FOIA requests, as set out below in 190-2.2(2), should be followed.

(2) The time limits dictated by the FOIA are as follows:

(a) Within ten working days upon receipt of a valid request, i.e., one that contains sufficient descriptive information, and the authorization of living third party when necessary, provided no unusual circumstances exist; or

(b) Within no more than ten additional working days, upon written notice of extension to requester, where there exists a need to collect records from offices other than the one receiving the request, the need to collate voluminous records for a single request exists, or consultation with another agency is required.

(3) While it is recognized that these time limits may be difficult to meet in all instances, acknowledgment of the request and some indication of whether records exist that will be reviewed for possible disclosure should be made within ten working days after receipt of the request.

(4) Should the request involve a highly sensitive covert investigation, contact the Training, Research, and Field Coordination Unit, FOIPA Section, FBIHQ, by secure telephone or teletype for direction before acknowledgment.

[190-2.3 Searching Procedures

[(1) An FOIPA request sent to a field office should be considered [to be a request for records in the Central Records System, unless another [system of records is specifically mentioned in the request. The fact that the [requester directed the request to a specific field office raises the

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

presumption that only records of that office are of interest to the requester. Thus, while a computer search might indicate that another field office or FBIHQ has information about the subject of the request, only information entered into the computer by the field office to which the FOIPA request was directed should be considered. Also, there is normally no processing of the computer printout for an FOIPA requester, unless it contains information in addition to that maintained in the source document or unless there is no source document.

(2) In response to FOIPA requests for records in the Central Records System, a field office must search the indices and other means by which it retrieves information from this system of records, including:

(a) the general indices, both manual and automated;

(b) automated investigative support systems, such as the Organized Crime Information System (OCIS), the Investigative Support Information System (ISIS), and the Intelligence Information System (IIS); and

(c) [a] microcomputer [data base] currently being operated by the field [division] must be searched if a comparison of the specific FOIPA request with the list of microcomputer data bases indicates that a specific data base could reasonably be expected to contain responsive information.]

(3) The Information Systems Administrator (ISA) will furnish a [list] of microcomputer data bases (see Part II, Section 16-18.4 (3)(a)) to the Field Privacy Control Officer (FPCO) and inform the FPCO [whenever] a microcomputer data base is to be added to or removed from the list. [The ISA is responsible for providing the FPCO with a list of microcomputer data bases which shall be current, have a revision date, include the case caption and/or an indication of the subject matter and type of investigation being conducted, and indicate whenever full-text retrieval capabilities have been or are being used.]

(4) [The FPCO will identify the system of records with which the microcomputer data base is associated and will ensure that the appropriate microcomputers are searched in response to FOIPA requests. When full-text retrieval capabilities are being used on the data base to be searched, in accordance with section (2)(c) above, the FPCO must determine if a full-text retrieval search of the data base is required for the FOIPA request. Full-text retrieval is used in a limited number of cases as an investigative technique to collate, analyze, and retrieve information. It is not part of the normal search process and is not used as a substitute for the general indices or the automated investigative support systems. However, if, at the time an FOIPA request is received, full-text retrieval capabilities are being used to retrieve information about individuals by name or personal identifier, a full-text retrieval search of that data base should be considered. In such cases, it may be appropriate to contact the requester before the search is conducted to determine if the requester is willing to pay the actual direct costs of conducting the search (see 28 CFR 16.10 and 16.47).]

[(5)] A microcomputer [data base] used exclusively in connection with a system of records other than the Central Records System, such as the Elsur Index or the National Center for the Analysis of Violent Crime, need be searched only in response to a request involving the other system of records.

190-2.4 Filing Procedures, Classification 190

(1) In order to preserve and maintain accurate records concerning the handling of a request submitted pursuant to the FOIPA, a separate correspondence-type file in the 190 classification is to be initiated at such time as it is determined that records are being maintained which pertain to the requester or to the subject matter which has been requested; however, a separate 190 file should not be opened if an exclusion (one of the tip-off provisions) is being used and no records are being released. Such a file can be opened when searching procedures determine the existence of records under the requester's name, even though it might be determined at a later time that those records are not identical with the requester.

(2) Where the initial search fails to locate the existence of possibly identifiable information or when a tip-off provision is used to exclude all the information about the subject of the request, the incoming

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

request letter and the response are to be maintained in the 190-0 or in a 190 control file, rather than in a separate, substantive file. This 190 file can also be utilized to maintain copies of correspondence where the only action by the field office is to forward the request to FBIHQ.

(3) The handling of all documents concerning the use of the tip-off provisions should be [in accordance] with procedures for the maintenance of the classified and informant information these documents often contain.

190-2.5 Field Office Records Referral Procedures

(1) The field office receiving a request for access to FBI records must determine what records (files) are responsive to the request. Existing Bureau instructions will determine where the records are processed, i.e., at FBIHQ, at the office receiving the request, or at the office of origin (OO).

(2) All main files which show the investigation was reported to FBIHQ will be processed at FBIHQ. Unreported main files will be processed by the OO. All "see" references normally are processed by the office receiving the request. Where the request is referred to FBIHQ, the FOIPA Section, [IMD,] will process the main file records, not only in the FBIHQ file, but also in the files of the office receiving the request and/or the OO, which are responsive to the request.

190-2 Seeking Access in Person

When a Privacy Act request is presented to a field office in person, the requester should be advised to put the request in writing or to complete an FD-706, after which the field office will process the request pursuant to the same time limits pertaining to requests received by mail. Should the individual wish to return to the field office to personally review processed documents, when available, it should be permitted. In addition, the requester is permitted to have one other person accompany him/her, providing the requester furnishes a statement authorizing a discussion of his/her personal records in the presence of this other individual. An FBI employee is to be present at all times during the requester's review of copies of FBI records in FBI space.

190-2.7 Consultation and Referral to Other Agency

(1) Where material to be released includes information previously obtained from another Federal agency, that agency is to be consulted prior to release of the information.

(2) Where the material being considered for release includes copies of the original documents obtained from another Federal agency, said documents will be referred to that agency whether on local or headquarters level. The field office should inquire at the local office of the Federal agency as to the proper disposition of the referral.

190-3 CONDITIONS OF DISCLOSURE

190-3.1 Written Authorization By Subject

The Privacy Act prohibits disclosure of personal information, with certain exceptions, to any person or other agency unless specifically authorized in writing by the person to whom the record pertains.

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

190-3.2 Exceptions

The Act provides for twelve exceptions to this disclosure prohibition. The exceptions used most often by the FBI in disseminating information from the central records system are:

(1) Information from FBI files may be disseminated as a proper "routine use" without the subject's authorization to any Federal Executive Branch agency to the extent the information is relevant to an authorized function of such agency. Information also may be disclosed as a routine use to a member of the Federal Judiciary if considered relevant to an authorized function of the recipient. In addition, information may be disclosed to a state or local criminal justice agency for an legitimate law enforcement purpose. ("Routine Use" is defined in the Privacy Act as the use of such record for a purpose which is compatible with the purpose for which it was collected.) Such a routine use dissemination does not constitute any change in past policy or procedures as the FBI always has been authorized to disseminate its records to other Government agencies for official business only. Such dissemination will continue under this new routine use procedure.

(2) Background and descriptive information on Federal fugitives is disseminated as a routine use to the general public and the news media to assist in the apprehension of the fugitives.

(3) News releases are disseminated as a routine use to the general public and the news media concerning apprehensions and other accomplishments.

(4) Public source information is similarly disseminated as a routine use on a continuing basis.

(5) Information is disclosed to private individuals and/or organizations when necessary to solicit information or cooperation for an authorized purpose, i.e., when it is necessary during the course of an official investigation to seek information from private individuals such as their observations, descriptions, or account of events which transpired. In such instances it might be necessary to disclose the nature of the crime of which the subject was suspect or similar personal information about the subject. Also, information may be disclosed to the private sector to the extent necessary to protect life or property.

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

190-3.3 Accounting of Disclosures

(1) Each time a record pertaining to an individual is disseminated to a person or other Federal, state, local, or foreign agency, whether orally or by any type of communication, written or electronic, an accounting of such dissemination, consisting of the date, nature, and purpose of each disclosure as well as the name and address of the person or agency to whom the disclosure is made, must be maintained for at least [six] years or the life of the record, whichever is longer, following the disclosure.

(2) The Act provides for access by the individual subject-requester to the accounting of disclosure made of records pertaining to him/her. Normally, the FBI will release this accounting to the individual at his/her request; however, the FBI is exempt from this particular statutory requirement and, where circumstances so dictate, the FBI will deny such a request, e.g., where dissemination was of a sensitive nature to an agency such as National Security Agency, Central Intelligence Agency or Drug Enforcement Administration.

190-4 INFORMATION COMPILED FOR CIVIL LITIGATION

(1) The Privacy Act does not permit an individual access to any information compiled in reasonable anticipation of a civil action or proceeding brought either by the Government or against the Government.

(2) In order for information to be denied a requester based on this provision, Office of Management and Budget (OMB) has indicated the civil action actually must have been filed so that the agency is on notice, as the original intent of this provision is to protect information collected by or at the request of the Office of the USA in preparation for civil litigation brought by or against the Government.

190-5 REQUIREMENTS IMPOSED BY THE PRIVACY ACT

(1) Only that information about an individual which is relevant and necessary to accomplish a purpose authorized by statute, Executive order of the President, or by the Constitution is to be recorded in FBI files.

(2) When interviewing an individual in an applicant- or civil-type investigation to solicit information about that individual, himself/herself, and not about someone else, the individual must be apprised in writing, of:

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

(a) The authority, whether by statute or Executive Order, which authorizes solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(b) The principal purpose for which the information is intended to be used;

(c) The routine use which may be made of the information;

(d) The effects on the interviewee, if any, of not providing all or any part of the requested information.

(3) Written forms containing the above information in all of the suitability- and civil-type classifications are maintained in each field office. At the termination of the interview, the form should be left with the interviewee. [Note: This requirement is not necessary in those applicant matters which are referred to the FBI by another agency or department, including the Department of Justice. The FBI conducts the interviews in these instances with the understanding that the referral agency or department notifies each person it solicits information from of the Privacy Act requirements described in subparagraph (2).]

(4) All information about an individual is to be maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness in any determination made concerning the individual based on such information. Only information meeting these four standards should be disseminated to other agencies.

190-5.1 Restrictions on Information Relating to First Amendment Rights

(1) The FBI is prohibited from maintaining records describing how any individual exercises rights guaranteed by the First Amendment unless authorized by statute or by the individual, or unless the particular record is pertinent to and within the scope of an authorized law enforcement activity.

(2) This restriction prohibits the collection, maintenance, use or dissemination of information concerning an individual's religious or political beliefs or activities, or membership in associations or organizations, unless:

(a) The individual has volunteered such information for [[his/her]own benefit;

(b) The information is expressly authorized by statute to be collected, maintained, used, or disseminated; or

(c) The activities involved are pertinent to and within the scope of an authorized investigation, adjudication, or correctional activity.

190-6 CRIMINAL PENALTIES

190-6.1 Unauthorized Disclosure

[Any officer or employee of any agency, who by virtue of [his/her] employment or official position, has possession of, or access to, agency records which contain individually identifiable information, the disclosure of which is prohibited by this Section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

190-6.2 Unpublished Records System

Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of the Act shall be guilty of a misdemeanor and fined not more than \$5,000.

190-6.3 Use of False Pretenses

Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

190-6.4 FBI Jurisdiction

The FBI has been designated by the Department of Justice as the agency having jurisdiction to investigate violations of the Privacy Act, [described above. The classification is 187, Privacy Act[of 1974]- Criminal.

190-7 PROMISE OF CONFIDENTIALITY

190-7.1 When Applicable

(1) In applicant, background-type investigations and investigations involving civil matters, as well as administrative inquiries, individuals interviewed in order to solicit information about someone other than the interviewee have a right to request from the FBI an express promise that the identity of the interviewee will be held in confidence. Such a promise is not to be encouraged, but granted on a selective basis when it is the only means to secure the information from the individual being interviewed.

(2) All individuals from whom information is sought in applicant- and civil-type cases must be apprised not only of the purpose for which the information is sought, as well as the uses to be made of the information; but also of the provisions of the Privacy Act regarding access to records and the allowance for confidentiality.

[(3) At what point in the interview process the person interviewed should be told of the Privacy Act and given the opportunity to request confidentiality is left to the best judgment of the interviewing Agent. [However, in almost every case, the logical time is at the beginning of the [interview to avoid the appearance of intentionally misleading or misinforming [the person interviewed. Where confidentiality is requested, the person being [interviewed should be assured any information he or she provides, which could [identify them as the source, will be withheld from anyone requesting access to [the records under the Privacy Act or the Freedom of Information Act.]

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

190-7.2 Recording of Promise of Confidentiality

[Where such an express promise has been requested and granted, it is absolutely imperative this fact be clearly recorded along with the results of the interview. Failure to note the interviewee was granted an express promise of confidentiality will result in the disclosure of the interviewee's identity to the subject of the investigation upon the latter's request to review the results of the investigation in accordance with the Privacy Act.

190-7.3 Types of Confidentiality

[A promise of confidentiality, when furnished to a source of information, may pertain to any one of three areas:

[[(1)] Source's identity to be concealed only from the subject of the investigation.

[[(2)] Source's identity not to be unnecessarily revealed until such time as the information is required in a judicial proceeding or administrative hearing.

[[(3)] Source's identity is to be concealed from anyone outside the FBI, in which case the use of "T" symbols should be employed in all communications prepared for dissemination.

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

190-7.4 Custodian of Records

The express promise of confidentiality may also be furnished on request to a state or local custodian of records, e.g., police department, private corporation, credit bureau, in applicant- and civil-type investigations. The custodian must be made aware that this is the only procedure which will afford adequate confidentiality to his/her agency.

190-8 USE OF SOCIAL SECURITY ACCOUNT NUMBER (SSAN)

190-8.1 Restrictions

(1) No Federal, state or local agency shall deny an individual any right, benefit or privilege provided by law because of the individual's refusal to disclose his/her SSAN except:

(a) A disclosure required by Federal statute, or

(b) A disclosure to a Federal, state or local agency maintaining a system of records in existence prior to 1/1/75, if such disclosure was required under statute or regulation adopted prior to that date to verify the identity of the individual.

(2) When requesting an individual to furnish SSAN, ensure that the individual be apprised of whether such disclosure is voluntary or mandatory, the statutory or other authority for its solicitation, and what uses will be made of it.

(3) There is no statutory provision for enforcement of this requirement; therefore, the FBI is not authorized to conduct an investigation of alleged violations by Federal, state or local agency personnel.

190-9 EMPLOYEE STANDARDS OF CONDUCT

[Except to the extent permitted pursuant to the Privacy Act, employees of the FBI shall:

[[(1)] Collect no information of a personal nature unless authorized to collect it to achieve a function or carry out a responsibility of the FBI;

[[(2)] Collect only that information which is necessary to FBI functions or responsibilities;

[[(3)] Collect information, wherever practicable, directly from the individual to whom it relates;

PART I

SECTION 190. FREEDOM ON INFORMATION-PRIVACY ACTS (FOIPA)

- [[(4)] Inform individuals from whom information (about themselves) is collected, of the authority for collection, the purposes thereof, the uses that will be made of the information, and the effects both legal and practical, of not furnishing the information;
- [[(5)] Neither collect, maintain, use, nor disseminate information concerning an individual's religious or political beliefs or activities or his/her membership in associations or organizations, unless, (i) the individual has volunteered such information for his/her own benefit; (ii) the information is expressly authorized by statute to be collected, maintained, used, or disseminated; or (iii) the activities involved are pertinent to and within the scope of an authorized investigation, adjudication or correctional activity;
- [[(6)] Advise their supervisors of the existence or contemplated development of any record system which retrieves information about individuals by individual identifier;
- [[(7)] Wherever required by the Act, maintain an accounting, in the prescribed form, of all dissemination of personal information outside the Department, whether made orally or in writing;
- [[(8)] Disseminate no information concerning individuals outside the Department except when authorized by Title 5, USC, § 552a, or pursuant to a routine use published in the Federal Register;
- [[(9)] Maintain and process information concerning individuals with care in order to ensure that no inadvertent disclosure of the information is made either within or without the Department; and
- [[(10)] Call to the attention of the field office Privacy Control Officer any information in a system maintained by the FBI which is not authorized to be maintained under the provisions of the Privacy Act of 1974, including information on First Amendment activities and information that is inaccurate, irrelevant or so incomplete as to risk unfairness to the individual concerned. The field office Privacy Control Officer should then consider the appropriate action to be taken after consultation with FBIHQ where necessary.

190-10 SYSTEMS OF RECORDS-NOTICE REQUIREMENTS

190-10.1 Definitions

- (1) Record - a documentary or computer record containing personal information identifiable with a U.S. citizen or permanent resident alien.
- (2) System of records - a group of "records," under the control of the FBI, from which information is retrieved by name or other personal identifier.

190-10.2 Notice Requirements

- (1) The Department of Justice, like every Executive Branch agency, must publish in the Federal Register a complete description of each system of records maintained by each component of the Department (system notice).

PART I

SECTION 190. FREEDOM OF INFORMATION-PRIVACY ACTS (FOIPA)

(2) For the FBI, the Department has published notices of several records systems, including National Crime Information Center (NCIC), Identification Division Records System, and the Central Records System.

(3) The FBI Central Records System is comprised of the over 200 classifications of investigative, administrative and correspondence files maintained at FBIHQ, all FBI field divisions, and the Legal Attache offices abroad. Information is retrieved from the Central Records System by means of manual and/or automated indices in each location at which the records are stored.

190-10.3 Noncompliance

Maintaining a system of records, as described above, independent of published FBI systems, without meeting the notice requirements, can subject the FBI to civil liability and the responsible FBI official or employee to criminal prosecution (see 190-6.2).

190-10.4 Special Indices Relating to Individual Major Investigations

(1) [The]FBI can maintain a separate index or listing, containing individually retrievable personal information, only by publishing a system notice in the Federal Register, or making the information also retrievable through[a search of]the Central Records System (GAO Report to the Comptroller General, 12/26/77).

(2) Making information[about an individual]retrievable through a search of the Central Records System is accomplished by[making the individual's name or personal identifier retrievable in the general indices, in an automated investigative support system, or in a microcomputer searched under the procedures described in 190-2.3.]

(3) If the information[to be]maintained separately[(e.g., in a microcomputer)]is only duplicative of that which was previously[made equally retrievable through the Central Records System, the information is already part of the Central Records System and no additional action need be taken.]